PATENT ABSTRACTS OF JAPAN

(11)Publication number : **11-272681**

(43)Date of publication of application : **08.10.1999**

(51)Int.CI. G06F 17/30
G06F 12/00

(21)Application number : **10-069744**

(22)Date of filing : **19.03.1998**

(71)Applicant : **HITACHI INFORMATION SYSTEMS LTD**

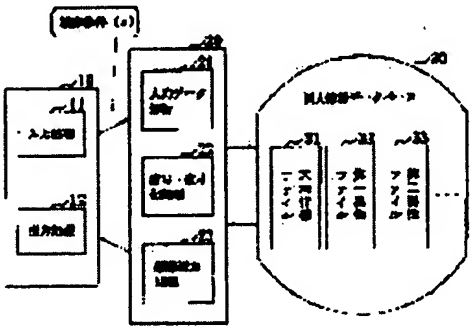
(72)Inventor : **MATSUURA TORU**
ISHIKAWA YORIO

(54) RECORDING METHOD FOR INDIVIDUAL INFORMATION AND RECORD MEDIUM THEREOF

(57)Abstract:

PROBLEM TO BE SOLVED: To perform a retrieval and an arithmetic process without spoiling processing performance in the case of normal access, but disabling a person who is not permitted to decipher individual information or acquire the whole information even when reading it out of an individual information data base.

SOLUTION: Information is divided into a basic information file 31 consisting of basic data items of individual information and attributes information files 32, 33... consisting of other attribute data items and the files are related by using individual codes which specify pieces of individual information as they are or codes ciphered by using cipher keys different by the files. For normal retrieval by a client 10, retrieval conditions are analyzed by an input data analysis part 21 and when 2 files are objectives, a ciphering and deciphering process part 22 decipher the ciphered individual codes by the files, performs retrieval from other files by ciphering them by the files, and performs an editing and output process 23.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of

rejection]
[Date of requesting appeal against examiner's decision of rejection]
[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平11－272681

(43)公開日　平成11年(1999)10月８日

(51)Int.Cl.[6]		識別記号	ＦＩ		
Ｇ０６Ｆ	17/30		Ｇ０６Ｆ	15/40	３４０
	12/00	５０５		12/00	５０５
				15/40	３２０Ｂ
					３７０Ｚ

審査請求　未請求　請求項の数７　ＯＬ　（全８頁）

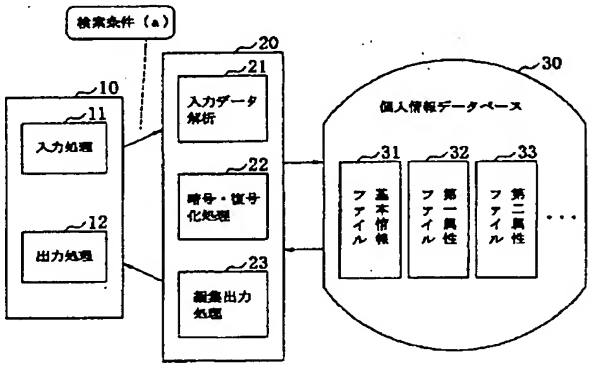
(21)出願番号　特願平10－69744

(22)出願日　平成10年(1998)３月19日

(71)出願人　000152985
株式会社日立情報システムズ
東京都渋谷区道玄坂１丁目16番５号
(72)発明者　松浦　徹
東京都渋谷区道玄坂一丁目16番５号　株式会社日立情報システムズ内
(72)発明者　石川　頼雄
東京都渋谷区道玄坂一丁目16番５号　株式会社日立情報システムズ内
(74)代理人　弁理士　磯村　雅俊　（外１名）

(54)【発明の名称】　個人情報の記録方法およびその記録媒体

(57)【要約】
【課題】個人情報データベースに対して、許可されない者が個人情報を読み出しても、その解読を不可能にするか、あるいは全体情報の取得を不可能にし、正常なアクセスの場合には処理性能を損うことなく、検索や演算処理を行える。
【解決手段】個人情報の基本データ項目からなる基本情報ファイル３１と、それ以外の属性データ項目からなる属性情報ファイル３２，３３，・・とに分割し、各個人情報を特定する個人コードをそのままないしはファイル毎に異なる暗号鍵を用いて暗号化したコードで、ファイルを関連付ける。クライアント１０から正常に検索するには、検索条件を入力データ解析部２１で解析し、２つ以上のファイルにまたがる場合には、暗号・復号化処理部２２でファイル毎の暗号化個人コードを復号し、ファイル毎に暗号化して他ファイルを検索し編集出力（２３）する。



【特許請求の範囲】
【請求項１】　コンピュータシステムで処理可能な記録媒体に個人情報を記録する記録方法において、
上記個人情報を、氏名、性別等の基本データ項目からなる基本情報を格納した基本情報ファイルと、該基本データ項目以外の属性データ項目からなる属性情報を格納した１個以上の属性情報ファイルとに分割してそれぞれ記録し、
各個人情報を特定する個人コードで上記基本情報ファイルと１以上の属性情報ファイルとを関連付けることを特徴とする個人情報の記録方法。
【請求項２】　請求項１に記載の個人情報の記録方法において、
前記個人コードは、さらに各基本または属性情報ファイル毎に異なる暗号鍵を用いてそれぞれ暗号化された個人コードであることを特徴とする個人情報の記録方法。
【請求項３】　コンピュータシステムで処理可能な記録媒体に個人情報を記録する記録方法において、
入力された検索条件を解析して基本情報ファイルまたは属性情報ファイルのいずれの検索であるかを判別し、
判別された第１の情報ファイルに対して上記検索条件により第１の検索を行い、　２つ以上の情報ファイルにまたがって検索が必要な場合には、上記第１の検索で得られた検索キーである鍵暗号化個人コードを復号化して、本来の個人コードを取得し、
判別された第２の情報ファイルに対して上記検索条件により第２の検索を行い、　さらに判別された第３の情報ファイルに対しても同じ処理を行い、
検索した結果を編集することを特徴とする個人情報の記録方法。
【請求項４】　個人情報を記録したコンピュータシステムで処理可能な記録媒体において、
上記個人情報を、個人情報の基本データ項目からなる基本情報ファイルと、該基本データ項目以外の属性データ項目からなる１個以上の属性情報ファイルとに分割して記録し、かつ各個人情報を特定する個人コードで上記基本情報ファイルと１個以上の属性情報ファイルとを関連付けた各情報ファイルの内容を記録したことを特徴とする個人情報の記録媒体。
【請求項５】　請求項４に記載の個人情報の記録媒体において、
前記個人コードは、さらに各基本または属性情報ファイル毎に異なる暗号鍵を用いてそれぞれ暗号化された個人コードである場合の各情報ファイルの内容を記録したことを特徴とする個人情報の記録媒体。
【請求項６】　請求項３に記載の各処理動作をプログラムに変換し、変換された該プログラムを記録したことを特徴とする記録媒体。
【請求項７】　バックアップのために外部記録媒体に記録保管する個人情報記録媒体において、
上記個人情報の全体を暗号鍵で暗号化し、かつその暗号化された個人情報を、基本情報ファイルと、１つ以上の属性情報ファイルとに分割し、各情報ファイルを暗号化された個人コードで関連付けたことを特徴とする個人情報を記録した外部記録媒体。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、コンピュータシステムにおいて、個人情報ファイルの機密保護を図ることが可能な個人情報記録方法、およびその方法で記録され、コンピュータにより読み出し可能な記録媒体に関する。
【０００２】
【従来の技術】最近、金融機関における個人情報の漏洩、あるいは市町村における住民情報の漏洩が問題となったニュースが報道されている。これは、コンピュータ化の発展により、コンピュータシステムで処理される個人情報が増加していることが原因である。一方、パソコン通信やインターネット等の普及によりコンピュータシステムの利用者がますます増加しており、パソコンを利用した預金者、あるいは住民からのデータベースへのアクセス要求は、今後増加する傾向にある。このような状況において、コンピュータシステムに蓄積されている各種個人情報は、プライバシー保護の観点から十分な機密保護の仕組みが要求されている。このような社会的な要求に対して、データの機密保護のための対策としては、例えばパスワードによるアクセス者の権限チェック、通信ネットワーク上のデータの暗号化処理、コンピュータシステムの外部記憶媒体に作成・保管するデータに対する暗号化処理、等が一般に行われている。
【０００３】個人情報の機密保護に関する従来技術としては、例えば、特開昭６４－１４６６５号公報に記載の市町村業務における住民基本台帳ファイル方式がある。この方式では、オンラインシステムを使用して個人データの登録や蓄積を行った住民基本台帳から、個人情報が外部に漏出することを防止するものであって、図２に示すように、磁気ディスク上のデータベースの暗号化を行う方式である。すなわち、住民基本台帳ファイル５５に対して入力端末装置５１から住民基本台帳データを入力する時に、暗号処理部５４であらかじめ定めた暗号鍵により前記住民基本台帳データを全て暗号化してからファイル５５に格納するものである。一方、住民基本台帳ファイル５５のデータに対して検索や演算を行う場合には、暗号処理部５４で復号処理した後に、住民基本台帳処理部５３で検索または演算処理を行い、処理結果を出力端末装置５２に出力する。
【０００４】
【発明が解決しようとする課題】前記公報に記載の従来技術においては、記録、蓄積されている個人情報である住民基本台帳ファイルが、ファイルダンプなどの手段に

より読み出されて外部に漏出されても、データが暗号化されているために、何人もこれを解読できず、その結果として個人情報の外部漏出を防止することができる。しかしながら、コンピュータシステムの記録装置に記録されているこの住民基本台帳ファイルは、コンピュータシステムの各種業務処理プログラムによって検索処理の対象となるファイルである。検索対象ファイルのデータが暗号化されていると、復号してから演算処理や検索処理を行う必要があるため、多くの余分な時間を要するという問題がある。また、暗号化の方法によっては、検索不可の条件が生ずるという問題があり、個人情報は保護されても、正常なコンピュータ処理に支障を生じるため、実用にならないという問題がある。

【０００５】具体的には、個人情報を検索する際の検索方法としては、個人を特定するための基本的な検索である氏名、性別、年齢（生年月日）、住所等の基本項目を検索キーに利用する場合（基本項目検索）と、収入が一定額以上や年齢が一定年齢以上といった特定の属性に対する条件に合致した個人を抽出する場合（属性条件検索）が考えられる。いま従来の方法により、データ自体に暗号化処理を施した場合、その暗号化の方法によっては、正しい検索条件に合致するデータが抽出できないことが考えられる。例えば、年齢６０歳以上で、かつ年間所得額が２００万円以上の者を抽出する場合、属性情報の年齢と年間所得額の項目を暗号化したときには、その大小関係が保証されないことが発生する。従って、現実の個人情報システムでは、属性項目の暗号化は実用的ではないという結論になる。このように、従来の個人情報の暗号化処理方法では、検索時の処理性能を考慮していなかった。そこで、本発明の目的は、このような従来の課題を解決し、アクセスを許可されない者が、通常のアクセス手段以外の不正な何らかの手段、例えばファイルダンプの実行等により記録媒体から個人情報を読み出して入手したとしても、その個人情報の解読を不可能にし、かつ正常なアクセス処理の場合には、検索ロジックを複雑にせず、しかも検索処理時間を大幅に増大しないような個人情報の記録方法およびその記録媒体を提供することにある。

【０００６】

【課題を解決するための手段】上記目的を達成するために、本発明による個人情報の記録方法では、先ず個人情報をその基本情報ファイル（例えば、氏名、性別、生年月日、住所）と、複数の属性情報ファイル（例えば、第一属性ファイルの項目として学歴、出生地住所、既婚・未婚等、第２属性ファイルの項目として収入、持家の有無、資産総額、負債総額等）に分割することにより、各ファイル間の関連が遮断された、１つの論理的な個人情報データベースを作成する。次に、作成した個人情報データベースに対して、このように分割した個人情報（基本情報ファイルと各属性情報ファイル）間の関連を暗号化したユニークな個人番号、あるいは単なるコード番号で結合して、個人情報データベースを完成させる。また、個人情報を分割した格納した各情報ファイルの内容を記録媒体に記録させることにより、その媒体を携帯することにより、任意の場所で個人情報の検索・演算処理が可能となる。これにより、許可されない者が恣意的に前記個人情報データベースにアクセスしても、その内容と個人を特定することができない仕組みを構築する。また、磁気ディスク上に作成した前記個人情報データベースの元のデータを単純に外部磁気媒体にバックアップしたデータについても、本発明による個人情報ファイルの関連を遮断する処理と、従来からのデータ全体に暗号化を行う処理とを二重に行うことにより、さらに強力な情報の秘匿手段を構じることが可能になる。

【０００７】

【発明の実施の形態】以下、本発明の実施例を、図面を用いて詳細に説明する。図１は、本発明の一実施例を示す個人情報システムのブロック図である。図１において、１０はクライアント装置、２０はサーバ、３０は個人情報を蓄積した個人情報データベースである。クライアント装置１０は、入力処理機構１１と出力処理機構１２を備えている。サーバ２０は、入力データ解析機構２１、暗号・復号化処理機構２２、編集出力機構２３を備えている。個人情報データベース３０は、基本情報ファイル３１と複数の属性情報ファイル３２、３３、…を備えている。本発明においては、図１に示すように、個人情報データを基本データ項目からなる基本情報ファイル３１と、基本データ項目以外の属性データ項目からなる少なくとも１つ以上の属性情報ファイル３２，３３とに分割し、各個人情報を特定する個人コードまたは暗号化された個人コードでこれらの基本情報ファイル３１と属性情報ファイル３２，３３相互間の関連付けを行う。このように、単に格納するファイルを分割しただけでも、統一した個人情報を読み出すことが不可能となる。そして、コードがファイルから読み出されるまでは各ファイル間の関連を判別することができない。また、コードを暗号化することにより、個人情報の解読は完全に不可能となる。

【０００８】図３は、本発明の一実施例を示す個人情報ファイルの暗号化処理の説明図である。個人情報データベースの構造も、図３により明らかとなる。ここでは、個人コードを暗号化して、各ファイルの関連付けを行う方法について述べる。各個人に対応してユニークに付与される個人コードとして、本来の個人コードｘを入力する（ステップ１０１）。次に、個人コードｘに対して、基本情報ファイル３１、各属性情報ファイル３２、３３、…の各々について、それぞれ異なるように設定した暗号鍵Ｋ１、Ｋ２、Ｋ３…により暗号化処理を行う（ステップ１０２～１０４）。これにより、基本情報ファイル３１、各属性情報ファイル３２，３３…には、X

１、Ｘ２、Ｘ３、･･･なる暗号化後の個人コードが設定される(ステップ１０４～１０７)。この時、各個人コードＸ、Ｘ1、Ｘ２、Ｘ３･･･については異なる値となる（１０５ａ～１０７ａ）。しかし、同じ個人の情報という点では同一の個人情報である（等号参照）。同じようにして、全ての個人に対応してそれぞれユニークに付与された個人コードy,z,･･･を暗号鍵Ｋ１，Ｋ２，Ｋ３、･･･により暗号化して、Ｙ１，Ｙ２，Ｙ３，･･･等の暗号化後の個人コードを各情報ファイル３１，３２，３３内に設定する従って、個人情報データベース上に存在する基本情報ファイル３１、属性情報ファイル３２、属性情報ファイル３３･･･の関連において、仮に同一番号Ｙを各ファイルの個人コード検索のキーとして検索を実施しても（ステップ１０５ｂ～１０７ｂ）、検索結果は同一の者の個人情報とはならない（不等号参照）。これにより、個人コードをキーとして結合を図る通常の検索結果からは、正しい個人情報が取得できないことから、許可されない者が恣意的に情報を取得しようとした場合への対抗策を講じることができる。

【０００９】図４は、本発明の一実施例を示す個人情報データベースの検索動作のフローチャートである。図４により、クライアントから入力された検索条件をもとに個人情報データベースの検索例を述べる。クライアントから入力された検索条件ａは、入力データ解析機構２１により解析され（ステップ２０１）、検索条件より検索ファイルを決定する（ステップ２０２）。検索条件ａの内容を解析した結果、基本情報ファイル３１の検索に関わる場合には、基本情報ファイル３１を検索し（ステップ２１１）、属性情報ファイル３２の検索に関わる場合には、属性情報ファイル３２を検索し（ステップ２１２）、属性情報ファイル３３の検索に関わる場合には、属性情報ファイル３３を検索し（ステップ２１３）、さらに他の属性情報ファイルが存在する場合には同様の処理を行い、検索条件ａに対して何れかのファイル検索処理を実施する（検索ステップ４０）。検索条件ａが１つのファイルを検索するだけで終了する場合には、これで検索は完了する。しかし、検索条件ａが２つ以上のファイルを検索する必要がある場合には、上記検索処理において暗号化された個人コードＸ１，Ｘ２，Ｘ３,･･･を検索するとともに、以下の処理が必要となる。検索条件ａをもとに検索した結果（個人コードＸｎのレコード）から、もとの個人コードＸに関する情報全体を取得するために、個人コードXn（ｎ＝１～３のいずれか）に対して暗号・復号化処理（ステップ２２１～２２３のいずれか）で復号化を実行することにより、本来の個人コードであるXを取得する。例えば、検索条件ａが基本情報ファイル３１の検索に関わる場合には、基本情報ファイル３１の検索（ステップ２１１）で取得した個人コードＸ１を暗号・復号化処理で復号化することにより（ステップ２２１）、本来の個人コードＸを取得する（復号化ステップ４１）。

【００１０】次に、復号化により得られた個人コードXについて、検索ステップ４０で入力していないその他の個人情報を取得するための検索キーを求める。例えば、暗号・復号化処理（ステップ２２１）で復号化した場合には、事前に基本情報ファイル３１に対して基本情報ファイル３１の検索処理（ステップ２１１）については実行済みであるが、属性情報ファイル３２，３３･･･についての情報は新たに取得する必要がある。そこで、暗号・復号化処理で暗号化を実行することにより、属性情報ファイル３２，３３に対する検索キー（Ｘ２、Ｘ３･･･）を取得する（ステップ２２２，２２３）。同様にして、属性情報ファイル３２，３３以外のファイルに対する暗号・復号化処理についても、必要な検索キーＸ１，Ｘ２，Ｘ３を取得する（ステップ２２２，２２３）。（以上、暗号化ステップ４２）個人情報データベースを検索するための必要な検索キーＸ１、Ｘ２、Ｘ３･･･をもとに、検索ステップ４０で入力していないその他の個人情報を取得する。例えば、暗号・復号化処理（ステップ２２１）で復号化した場合には、事前に基本情報ファイル３１に対して基本情報ファイル検索の処理は実行済みであり（ステップ２１１）、残りの属性情報ファイル３２，３３･･･についての情報を新たに取得する必要がある。このため、個人コードＸ２、Ｘ３･･･を検索キーとして、属性情報ファイル３２，３３の検索を行う（ステップ２１２，２１３，･･）。同じようにして、属性情報ファイル３２，３３･･･についても、個人コードＸ２，Ｘ３を用いて検索を行う（ステップ２１１～２１３）（以上、検索ステップ４３）。これまでの検索結果を用いることにより、基本情報ファイル３１および属性情報ファイル３２，３３･･･の検索結果で得られた個人情報データを編集して（ステップ２０３）、クライアントに渡す。

【００１１】上記検索処理は、特定の検索条件ａが、基本情報ファイル３１、属性情報ファイル３２，３３，･･のうちいずれか１つのファイルに対して検索条件が適用できる場合、例えば氏名、性別、年令を格納している基本情報ファイル３１に対して検索条件ａとして、６０歳以上の女性を検索するとき等であり、複数ファイルの項目に対する検索条件となる場合、例えば住所、年収、資産を格納している属性情報ファイル３２と基本情報ファイル３１に対して検索条件ａとして、６０歳以上で年収３００万円の人を検索するとき等、の場合については、以下に説明する処理手順で実現できる。複数ファイルの項目に対する検索条件となる場合、例えば、基本情報ファイル３１と属性情報ファイル３２の複数項目を検索条件とする場合、先ず基本情報ファイル３１で検索抽出した個人情報のグループに対して、個人コードＸ１，Ｘ２を復号化して、復号化した結果を検索キーＸとして属性情報ファイル３２を検索する。その結果に対して複

数項目からなる検索条件をあてはめることにより、検索条件に該当する個人情報を抽出することが可能となる。さらに検索条件の内容として、属性情報ファイル３２，３３，・・の項目から検索条件を設定した時で、該当する個人情報のグループ全体について、抽出・集計する場合についても同様の処理手順で可能となる。例えば、属性情報ファイル３２の項目を検索条件として検索した個人情報のグループに対して、個人コードＸ２を復号化して、復号化した結果Ｘを検索キーとして、基本情報ファイル３１、属性情報ファイル３２･･･を検索する。検索した結果を編集することにより、検索条件に該当する個人情報のグループを抽出することが可能となる。その結果を集計することも可能となる。

【００１２】以上説明したように、個人情報ファイルの個々の属性項目に対してはデータを暗号化していないため、従来から使用している検索条件（等号関係、大小関係等）については、そのままの仕組みで検索処理を行なうことが可能となり、各ファイル間でのデータの関連については、個人コードの復号化と暗号化の仕組みにより従来と同じ検索処理が可能となる。なお、前述の実施例では、ファイルを分割して個人コードを分割した各ファイル毎に異なる暗号鍵を用いて暗号化した場合の検索方法について述べたが、他の実施例として、ファイルを分割して個人コード（暗号化しない）で分割された各ファイルを関連付けるだけでも、個人情報の秘匿保護を実現できる。この場合には、ファイルを検索して個人コードを検索しなければ分割された他のファイルがどれであるかが判別できないため、統一した個人情報を不正に取得することは困難となる。また、本発明においては、個人コードまたはファイル毎に異なる暗号鍵で暗号化された個人コードで分割された各ファイルを関連付けしたファイル内容を記録媒体に格納することにより、その記録媒体を携帯すれば、任意の場所において本発明を実施することができる。また、本実施例の検索方法の各ステップをプログラムに変換し、そのプログラムを記録媒体に記録することにより、その記録媒体を携帯すれば、任意の場所において本発明による検索を実施することができる。さらに、上述したような個人情報ファイルは、コンピュータシステムの不測の事故、故障、或いは不正アクセス等によりデータが破壊、または消滅されることから保護するために、必ず外部記憶媒体にバックアップ・ファイルとして記録保管される。そのような外部記憶媒体での個人情報は、直接検索対象のファイルではなく、従来の技術によりデータ自体を暗号化して得られたデータファイルである。　本発明では、データ全体を暗号化した上で、さらに前述の実施例のようにそのファイルを分割して、個人コードで関連付けることにより外部記憶媒体に記録すれば、そのデータ漏出に対する安全性がより高められる。

【００１３】このように、本実施例においては、個人情報を基本情報ファイルと幾つかの属性情報ファイルに分割して、その関連を結び付けるための個人コードをそのままないしは暗号化することにより、許可されない者が恣意的にデータを取出しても、暗号化の仕組みを公開しない限り取得した情報は無意味なものとなり、その結果、機密性を確保することができる。一方、許可された者がデータを取出す際には、暗号化の仕組みを利用することにより、通常の個人情報データベースを検索する場合とほぼ同程度の処理性能を確保することが可能となる。これは、個々の検索項目に対しては暗号化を行なっていないため、従来から使用している検索条件（等号関係、大小関係等）については、そのままの仕組みで検索処理を行なうことが可能となることによるものである。

【００１４】

【発明の効果】以上説明したように、本発明によれば、個人情報データベースに対して、アクセスを許可されない者が不正な方法で個人情報を読み出して入手しても、その個人情報の解読を不可能ないしは完全情報の取得を不可能にし、かつ正常なアクセスに対しては、その処理性能を損わずに個人情報に対して検索、演算することができるので、個人情報の秘匿を図ることができる。

【図面の簡単な説明】

【図１】本発明の一実施例を示す個人情報データベースシステムのブロック図である。

【図２】従来における個人情報データベースシステムの磁気ディスク上の暗号化の例を示す図である。

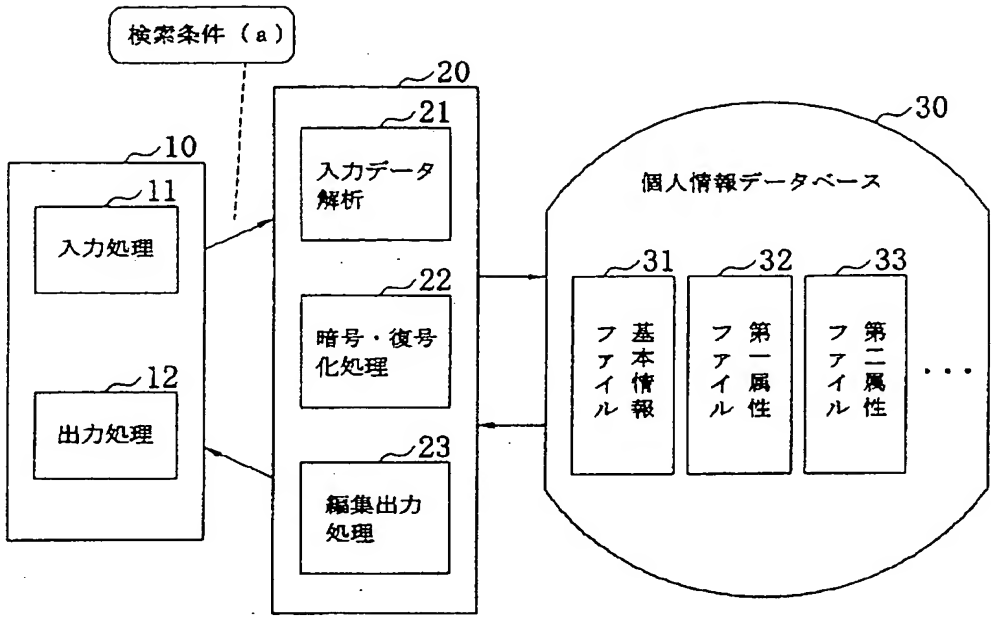
【図３】本発明の一実施例を示す個人情報データベースに対する暗号化処理のフローチャートである。

【図４】本発明の一実施例を示す個人情報データベースの検索処理のフローチャートである。

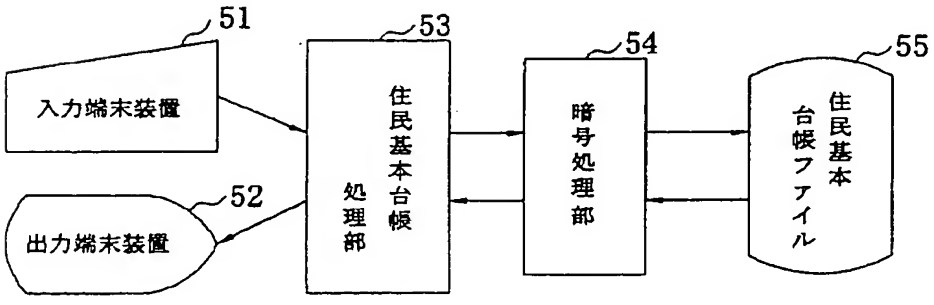
【符号の説明】

１０…クライアント装置、２０…サーバ、３０…個人情報データベース、１１…入力処理機構、１２…出力処理機構、２１…入力データ解析機構、２２…暗号・復号化処理機構、２３…編集出力機構、３１…基本情報ファイル、３２，３３…第１、第２属性ファイル、５１…入力端末装置、５２…出力端末装置、５３…住民基本台帳処理部、５４…暗号処理部、５５…住民基本台帳ファイル。

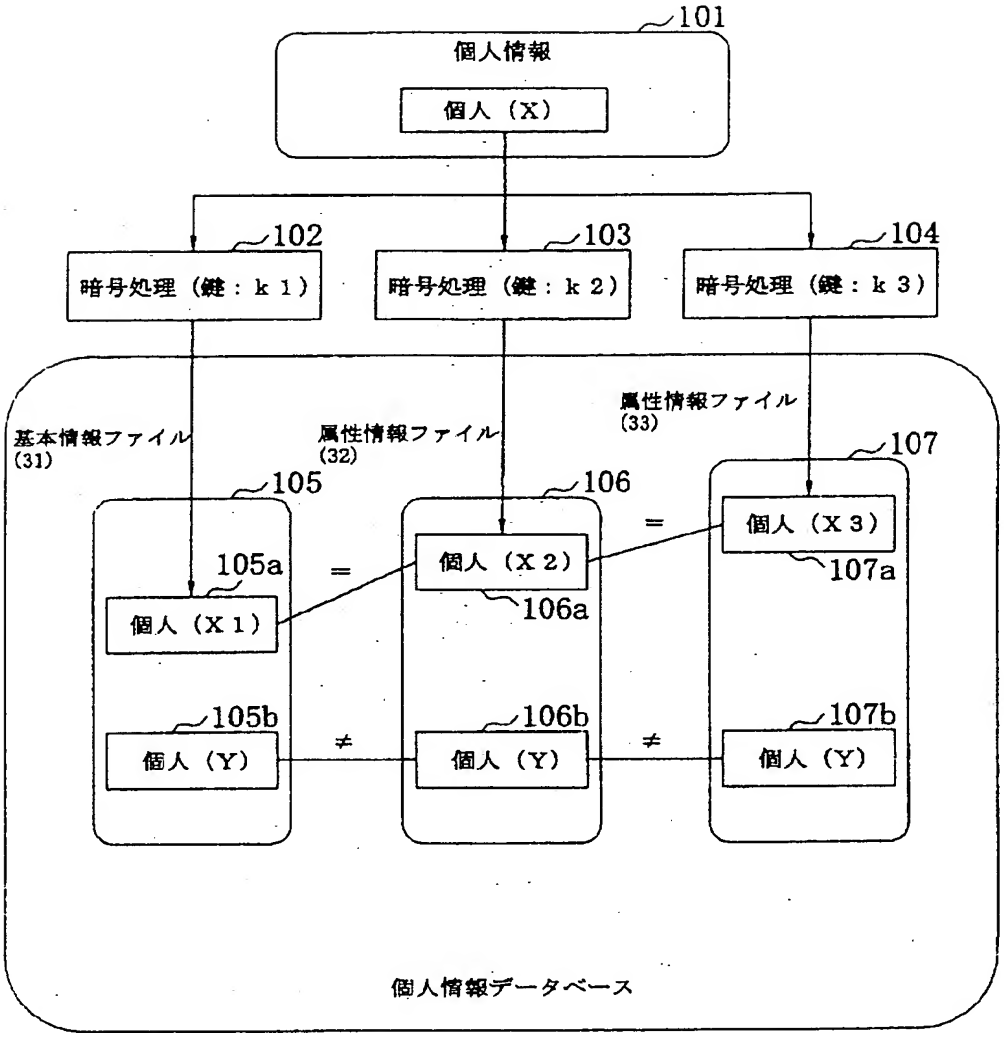
【図１】


検索条件（a）
10
11
入力処理
12
出力処理
20
21
入力データ解析
22
暗号・復号化処理
23
編集出力処理
30
個人情報データベース
31
基本情報ファイル
32
第一属性ファイル
33
第二属性ファイル
・・・

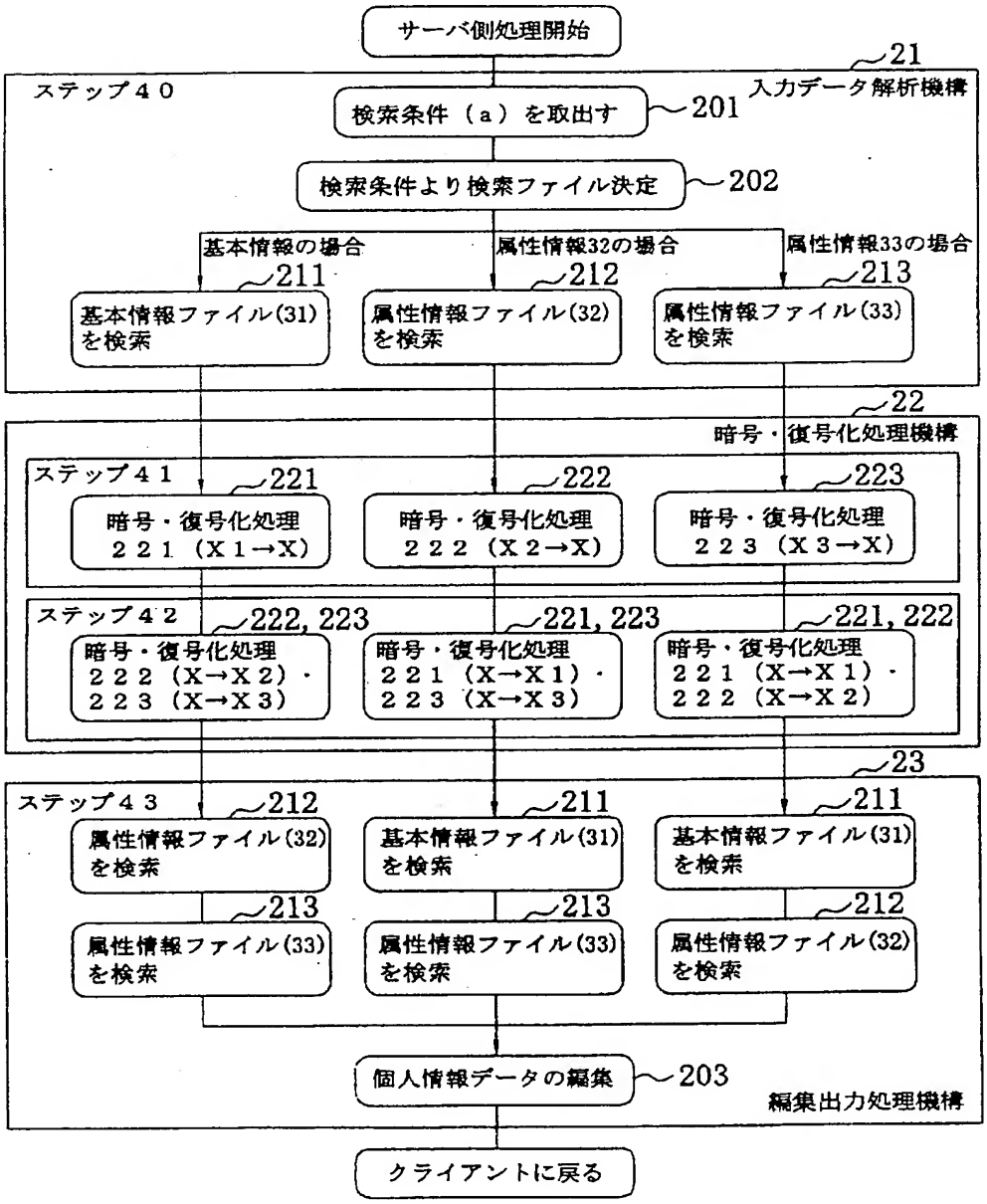
【図２】


51
入力端末装置
52
出力端末装置
53
住民基本台帳処理部
54
暗号処理部
55
住民基本台帳ファイル

【図3】


101
個人情報
個人（X）
102
暗号処理（鍵：k1）
103
暗号処理（鍵：k2）
104
暗号処理（鍵：k3）
基本情報ファイル
(31)
属性情報ファイル
(32)
属性情報ファイル
(33)
105
106
107
105a
個人（X1）
=
個人（X2）
106a
=
個人（X3）
107a
105b
個人（Y）
≠
106b
個人（Y）
≠
107b
個人（Y）
個人情報データベース

【図４】


サーバ側処理開始
21
入力データ解析機構
ステップ４０
検索条件（ａ）を取出す
201
検索条件より検索ファイル決定
202
基本情報の場合
属性情報32の場合
属性情報33の場合
211
212
213
基本情報ファイル(31)を検索
属性情報ファイル(32)を検索
属性情報ファイル(33)を検索
22
暗号・復号化処理機構
ステップ４１
221
222
223
暗号・復号化処理 ２２１（Ｘ１→Ｘ）
暗号・復号化処理 ２２２（Ｘ２→Ｘ）
暗号・復号化処理 ２２３（Ｘ３→Ｘ）
ステップ４２
222, 223
221, 223
221, 222
暗号・復号化処理 ２２２（Ｘ→Ｘ２）・２２３（Ｘ→Ｘ３）
暗号・復号化処理 ２２１（Ｘ→Ｘ１）・２２３（Ｘ→Ｘ３）
暗号・復号化処理 ２２１（Ｘ→Ｘ１）・２２２（Ｘ→Ｘ２）
23
ステップ４３
212
211
211
213
213
212
属性情報ファイル(32)を検索
基本情報ファイル(31)を検索
基本情報ファイル(31)を検索
属性情報ファイル(33)を検索
属性情報ファイル(33)を検索
属性情報ファイル(32)を検索
個人情報データの編集
203
編集出力処理機構
クライアントに戻る